



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/883,733	06/18/2001	Alexander E. Andreev	01-308 1496.00129	2457
24319	7590	08/11/2005	EXAMINER	
LSI LOGIC CORPORATION 1621 BARBER LANE MS: D-106 MILPITAS, CA 95035			LEMMMA, SAMSON B	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 08/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/883,733

Applicant(s)

ANDREEV ET AL.

Examiner

Samson B. Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 25 May 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 11 & 20 is/are rejected.
- 7) ☒ Claim(s) 2-10 and 12-19 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

Art Unit: 2132

## ***DETAILED ACTION***

1. This office action is in replay to an amendment filed on May 25, 2005.

**Claims 1-20** have been amended and **claims 1-20** are pending.

### ***Response to Arguments***

2. Applicant's arguments with respect to **claims 1-20** have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1,11 and 20** are rejected under 35 U.S.C. 102 (b) as being unpatentable over **Terry F. Ritter** (hereinafter referred to as **Ritter**) (U.S. Patent No. 5,623,549) in view of **Luyster** (hereinafter referred to as **Luyster**) (U.S. Patent No. 6,182,216 B1)

Art Unit: 2132

5. **As per claim 1, 11 and 20** Ritter discloses a method of defining a

transformation between an input signal and an output signal, the method comprising the steps of:

- (B) **Allocating said input signal** [Column 16, lines 64-65; Figure 10, ref. Num “106”](64 bit-input message block X is allocated) **among a plurality of block input signals**[Column 16, lines 65-66; Figure 10, ref. Num “183a”](the input message is allocated into eight message sub-blocks  $x_1, x_2, \dots, x_8$  where each  $x_i$  is an 8 bit sub-block of X);

- (C) Generating a **plurality of a block output signals responsive to said one of said block input signals and (ii) said symbol in one of said tables**; [Column 16, lines 66-column 17, lines 6; figure 10, ref. Num “182” shown above ref. Num “180”; ref. Num “180”; ref. Num “182” shown below ref Num “180”](Each of the blocks  $x_i$  is transformed first via corresponding substitution mechanism or transfer function as shown on figure 10, ref. Num “182” which is shown above ref. Num “180” to produce an 8 bit values  $x'_i$ . Then the 8-bit data values  $x'_i$  as a 64 bit data block goes to another transfer function which is the DES mechanism shown on figure 10, ref. Num “180” and using the **key K** produces a 64-bit output data block **Y** made up of 8-bit sub-blocks  $y_1, y_2, y_3, \dots, y_8$ . Finally each of the 8-bit sub-blocks  $y_i$  is transformed again by a substitution/transfer function block as shown on figure 10, ref. Num “182” below ref. Num “180” and produces 8-bit data block output  $y'_i$ )

- (D) **concatenating said block output signals to form said output signal of said circuit**. [Column 17, lines 6-8]

**Ritter** does not explicitly disclose

- copying a plurality of symbols from a source file to a plurality of tables of said circuit

However, In the same field of endeavor, **Luyster** discloses

Art Unit: 2132

- Copying a plurality of symbols from a source file to a plurality of tables (s-box) of said circuit [Column 15, lines 54-59 and column 4, lines 44-59] (block cipher to encrypt a large file and which nevertheless ensures that the subkeys generated by the method reflect every bit of the key in a complex uncorrelated manner before the encryption this files are loaded on the s-box or look up tables as explained on column 4, lines 50-59 and column 15, lines 54-59 meets the recitation of this limitation).

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of copying a plurality of symbols from a source file to a plurality of tables (s-box) as per teachings of **Luyster** into the method as taught by **Ritter** in order to provide a secure mechanism for transferring files for encryption them from the source files to the S-box (tables).

### ***Allowable Subject Matter***

Claims 2-10 and 12-19 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### ***Conclusion***

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2132

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

08/04/2005

*Justin T. Darrow*  
JUSTIN T. DARROW  
PRIMARY EXAMINER

Application/Control Number: 09/883,733

Page 6

Art Unit: 2132